(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平10－135943

(43)公開日　平成10年(1998)５月22日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｈ０４Ｌ　9/10		Ｈ０４Ｌ　9/00	６２１Ａ
Ｇ０６Ｋ　17/00		Ｇ０６Ｋ　17/00	Ｔ
Ｇ０９Ｃ　1/00	６６０	Ｇ０９Ｃ　1/00	６６０Ａ
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７５Ｄ
			６７５Ｂ

審査請求　未請求　請求項の数９　ＦＤ　（全９頁）

(21)出願番号　特願平8－299822

(22)出願日　平成８年(1996)10月25日

(71)出願人　000002897
大日本印刷株式会社
東京都新宿区市谷加賀町一丁目１番１号

(72)発明者　林　昌弘
東京都新宿区市谷加賀町一丁目１番１号
大日本印刷株式会社内

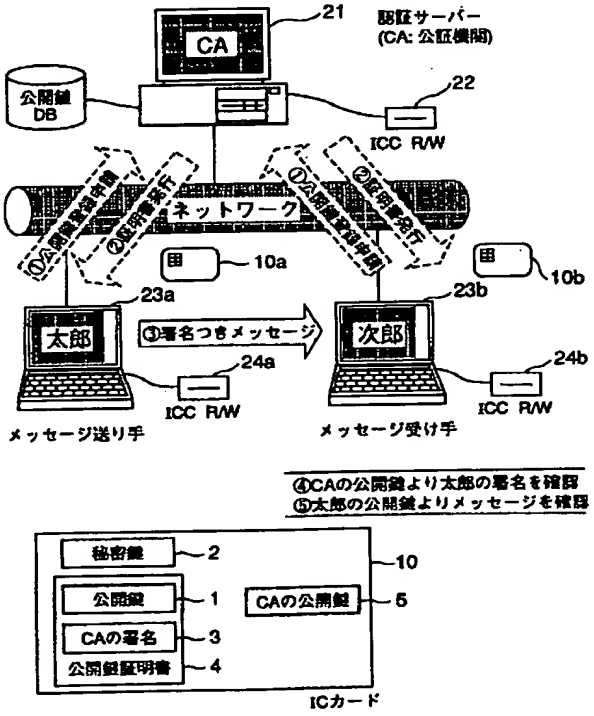
(74)代理人　弁理士　小西　淳美

(54)【発明の名称】　携帯可能情報記憶媒体及びそれを用いた認証方法、認証システム

(57)【要約】

【課題】　ネットワークでデジタル署名署等の認証に用いる鍵を安全に管理する。

【解決手段】　ＲＳＡ署名法等の公開鍵暗号方式の認証に用いる、各自の公開鍵１及び秘密鍵２を、公開鍵及び該公開鍵に対するＣＡ（公証機関）のデジタル署名３とからなる公開鍵証明書４と、秘密鍵として収容し、更にＣＡの公開鍵５も収容したＩＣカード１０を送り手及び受け手の双方で用いる。送り手はＣＡからオフラインで入手したＩＣカード１０ａをネットワーク端末にセットして、秘密鍵でデジタル署名を作成し、メッセージにデジタル署名と公開鍵証明書とを添付して受け手に送る。受け手では、ＣＡからオフライン入手したＩＣカード１０ｂ中のＣＡの公開鍵で、送られた公開鍵証明書のＣＡの署名を認証し、送り手の公開鍵を認証する。認証された送り手の公開鍵で送り手の署名を認証し、メッセージを認証する。



1

【特許請求の範囲】

【請求項１】　公開鍵暗号方式の認証に用いる少なくとも一対の公開鍵及び秘密鍵を、公開鍵及び該公開鍵に対する公証機関のデジタル署名とからなる公開鍵証明書と、秘密鍵として収容し、更に公証機関の公開鍵も収容した、携帯可能情報記憶媒体。

【請求項２】　収容された、秘密鍵、公開鍵証明書及び公証機関の公開鍵が、書換禁止属性を有する請求項１記載の記載の携帯可能情報記憶媒体。

【請求項３】　収容された秘密鍵が外部読出禁止属性を有し、外部より入力された原文を該秘密鍵を用いて媒体内部で暗号化して暗号文を出力する、請求項１又は２記載の携帯可能情報記憶媒体。

【請求項４】　携帯可能情報記憶媒体がＣＰＵとメモリを有するＩＣカードである、請求項１～３のいずれか１項に記載の携帯可能情報記憶媒体。

【請求項５】　収容された少なくとも一対の公開鍵及び秘密鍵が、ＲＳＡ署名法によるデジタル署名に用いる復号鍵及び暗号鍵である、請求項１～５のいずれか１項に記載の携帯可能情報記憶媒体。

【請求項６】　ネットワークで送り手が受け手に情報を送付する際に該情報の認証情報として利用する公開鍵暗号方式の公開鍵及び秘密鍵について、

送り手は、送り手の分の公開鍵及び秘密鍵と、公証機関の公開鍵とについて、公証機関から請求項１～４のいずれかに記載の携帯可能情報記憶媒体を取得する事で、送り手の公開鍵及び該公開鍵に対する公証機関のデジタル署名とからなる公開鍵証明書と、送り手の秘密鍵と、公証機関の公開鍵とを用意し、

送り手は受け手に上記秘密鍵で作成した認証情報とともに、上記公開鍵証明書を送付し、

受け手も、受け手の分の公開鍵及び秘密鍵と、公証機関の公開鍵とについて、公証機関から請求項１～４のいずれかに記載の携帯可能情報記憶媒体を取得する事で、受け手の公開鍵及び該公開鍵に対する公証機関のデジタル署名とからなる公開鍵証明書と、受け手の秘密鍵と、公証機関の公開鍵とを用意し、

受け手は、上記受け手の携帯可能情報記憶媒体に収容された上記公証機関の公開鍵と、送り手から送付された公開鍵証明書が有する公証機関のデジタル署名とを用いて、先ず該公開鍵証明書が有する送り手の公開鍵を認証し、次いで該認証された送り手の公開鍵と送り手から送付された認証情報とを用いて送付された情報を認証する、携帯可能情報記憶媒体を用いた認証方法。

【請求項７】　認証情報がＲＳＡ署名法によるデジタル署名である請求項６記載の携帯可能情報記憶媒体を用いた認証方法。

【請求項８】　送り手が受け手に情報を送付する際に、該情報に添付する認証情報に公開鍵暗号方式の公開鍵及び秘密鍵を用いる、ネットワークシステムの認証システムにおいて、

2

送り手及び受け手のそれぞれの端末は、送り手及び受け手のそれぞれの公開鍵及び秘密鍵、並びに公証機関の公開鍵について、公開鍵及び該公開鍵に対する公証機関のデジタル署名とからなる公開鍵証明書と、秘密鍵と、公証機関の公開鍵とを収容する請求項１～４のいずれかに記載の携帯可能情報記憶媒体をそれぞれ備え、

送り手は、送り手の携帯可能情報記憶媒体を用い、該携帯可能情報記憶媒体に収容された送り手の秘密鍵を用いて作成された認証情報と、該携帯可能情報記憶媒体に収容された送り手の公開鍵に対する公開鍵証明書を送付し、

受け手は、受け手の携帯可能情報記憶媒体を用い、該携帯可能情報記憶媒体に収容された公証機関の公開鍵と、送り手から送付された公開鍵証明書が有する公証機関のデジタル署名とを用いて、先ず該公開鍵証明書が有する送り手の公開鍵を認証し、次いで該認証された送り手の公開鍵と送り手から送付された認証情報とを用いて送付された情報を認証する、携帯可能情報記憶媒体を用いた認証システム。

【請求項９】　認証情報がデジタル署名である請求項８記載の携帯可能情報記憶媒体を用いた認証システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ネットワークにおける情報伝達の際に、認証に利用する鍵の管理をより安全に行う技術に関する。特に、デジタル署名等の認証に利用する公開鍵暗号方式の秘密鍵及び公開鍵を安全且つ効率的に管理する技術に関する。

【０００２】

【従来の技術】近年、ネットワークが情報伝達手段として普及し、ネットワーク上での商取引等のさらなる展開において、伝達する情報の正当性を担保できる技術が極めて重要な事項となっている。例えば、認証情報としてデジタル署名を添付する方法がある。図３はデジタル署名の説明図である。デジタル署名とは、メッセージの送り手がメッセージに添付する一種の証明書である。また、いわば従来の紙に対する捺印である。デジタル署名は、通常、メッセージ（原文）６を圧縮した圧縮文を送り手の暗号鍵で暗号化した暗号文７であり（なお、暗号化の対象となる原文はメッセージの全て又は一部でも良い。）、送り手の復号鍵で元の圧縮文に復号できる。つまり、受け手は、受け取ったメッセージから圧縮文を作成し、また受け取ったデジタル署名を復号化してもう一つの圧縮文を作り、これら二つの圧縮文が一致する事で受け取ったメッセージの内容が改ざんされてなく正しいものであると判断する。また、デジタル署名は、そのメッセージが確かに送り手本人によって作成されたものである事を証明するものでもある。すなわち、デシダル署名は、紙ベースであれば、伝達すべきメッセージが記載

された通知書に捺印された送り手の印鑑（の印影）であり、記載された内容の正当性と、記載内容が送り手によって作成されたものであると示すものである。従って、デジタル署名は、メッセージ認証とユーザ認証の両方の機能を有する。また、紙ベースの印鑑に対して、デジタル署名は電子印鑑でもある。

【０００３】ところで、暗号鍵と復号鍵とが同一の鍵、すなわち対象暗号の場合は送り手及び受け手が用いる鍵の両方を秘密鍵（秘密鍵暗号方式）とする必要がある。しかし、暗号鍵と復号鍵とが異なる非対称暗号の場合は、何方か一方のみを秘密鍵として他方を公表する公開鍵とすることができる（公開鍵暗号方式）。このような非対称暗号の一つとして、ＲＳＡ（Ｒｉｖｅｓｔ，Ｓｈａｍｉｒ，Ａｄｅｌｍａｎ）暗号系がある。ＲＳＡ暗号系は、一般に、暗号鍵を公開鍵に復号鍵を秘密鍵にするが、デジタル署名にＲＳＡ暗号系を用いる場合は、暗号鍵を秘密鍵に復号鍵を公開鍵にする。これをＲＳＡ署名法という。こうすれば、送り手が暗号化に用いる自分の鍵を秘密鍵として安全に保管すれば良く、その秘密鍵に対する復号鍵は公開鍵として公表しても安全だからである。これは、紙ベースで、実印を自分で安全に保管すれば良いのと同じである。

【０００４】ところで、紙ベースでも、捺印された印鑑（実印）の印影が送り手本人のものであることの確かな証明は、その実印の印影を有する印鑑（登録）証明書という、公的機関によって発行された書類によって印鑑証明がなされる。従って、実印を捺印した書類と、その実印が本人のものであるとことを証明する印鑑証明書が１セットになって、始めて、前記書類の正当性が確認される。これと同じ様に、デジタル署名でも、復号鍵を公開鍵とするには、信頼できる機関、すなわち公証機関（ＣＡ：Ｃｅｒｔｉｆｉｃａｔｉｏｎ　Ａｕｔｈｏｒｉｔｙ）が、その公開鍵を送り手本人のものに間違いないことを証明する手段が必要である。それが、公開鍵の証明書である。すなわち、紙ベースの印鑑証明書にに対して、電子印鑑証明書である。ところで、この公証機関による公開鍵証明書も、その公開鍵を一つの情報として捉えて、その情報（公開鍵）と、その情報に対する公証機関のデジタル署名とからなる。従って、送り手が受け手に送る、メッセージが今度は公開鍵であり、送り手が公証機関の場合に相当する。公証機関は、公証機関の秘密鍵で公証機関のデジタル署名を作成し、その公開鍵証明書を構成する公開鍵は、前記「公証機関の秘密鍵」と組の「公証機関の公開鍵」を用いて復号化して、認証することとなる。従って、送り手が受け手にメッセージ等の情報を送る際は、メッセージと共に、そのメッセージに対する送り手のデジタル署名と、そのデジタル署名からメッセージを認証する為の復号鍵と、その復号鍵が送り手本人のものであることを証明する公証機関の証明書（この証明書に前記復号鍵が含まれる）とを、送ることとなる。

【０００５】

【発明が解決しようとする課題】ところが、ＲＳＡ等の公開鍵暗号方式を認証に用いる場合、先ず自分の秘密鍵は厳重に管理することが必要だが、それをハードディスク或いはフロッピーディスク等の磁気ディスク等へ保管しても、第三者に不正にアクセスされ盗用や改ざんの危険性がある。また、復号鍵とする公開鍵は、公表する鍵のため盗用という問題はないが、改ざんに対しても公証機関の公開鍵証明書を取っておけば防御できる。しかし、取得した公開鍵証明書も秘密鍵と同様に磁気ディスク等に保管したものに不正にアクセスされて保管者の知らない内に改ざんされれば、証明書として機能しない。すなわち、受け手には不正な公開鍵証明書が送付される事になり、不正な証明書である事は判断できても、真正なものが送付されていないので、結局、送り手の情報は受け手には伝達されても、その情報が正当なものであるとの認証までは出来ず、情報伝達が行われないという事態が発生する。これは、公証機関による公開鍵証明書を用いたとしても、その公開鍵証明書を真正な状態に維持できなければ、情報伝達の安全性は確保できない事を意味する。これを紙ベースの印鑑証明書に例えれば、証明すべき印鑑の印影が改ざんされれば、印鑑証明書の真正さが失われる事に相当する。

【０００６】

【課題を解決するための手段】そこで、本発明では、上記課題を解決し目的を達成するために、デジタル署名等の認証に利用する公開鍵暗号方式の少なくとも一対の公開鍵及び秘密鍵を、公開鍵及び該公開鍵に対する公証機関のデジタル署名とからなる公開鍵証明書と、秘密鍵とを、携帯可能情報記憶媒体として例えばＣＰＵ内蔵のＩＣカードに収容すると共に、更に公証機関の公開鍵も収容したものとして利用する。送り手及び受け手の双方は、それぞれの分のＩＣカードをそれぞれ保持管理し、必要な時にカードリーダライタにセットして使えば、不正に第三者にアクセスされる危険性はなくなる。送り手の分のＩＣカードには、送り手の公開鍵及び秘密鍵について、送り手の公開鍵と該公開鍵に対する公証機関のデジタル署名とからなる送り手の分の公開鍵証明書、送り手の秘密鍵、公証機関の公開鍵が収容される。一方、受け手の分のＩＣカードにも同様に、受け手の公開鍵及び秘密鍵について、受け手の公開鍵と該公開鍵に対する公証機関のデジタル署名とからなる受け手の分の公開鍵証明書、受け手の秘密鍵、公証機関の公開鍵が収容される。

【０００７】また、上記ＩＣカードを用いた情報の認証方法は次の様にする。先ず、送り手は上記送り手の分のＩＣカードを公証機関からオフラインで入手し、情報を受け手に送るときは、該ＩＣカードに収容された送り手の秘密鍵でデジタル署名等の認証情報を作成し、この認

証情報とＩＣカードに収容された送り手の公開鍵証明書とを、送付したい情報とともに送る。受け手側でも、事前又は事後に、送り手と同様に、送り手と同一の即ち共通の公証機関から、受け手の分のＩＣカードをオフラインで入手して用意し、受け手のＩＣカードに収容された公証機関の公開鍵で、送り手の前記公開鍵証明書に含まれる送り手の公開鍵を認証し、認証された送り手の公開鍵と認証情報（例えばデジタル署名）で、送り手から送付された情報を認証する。

【０００８】また、送り手が受け手にネットワークで情報を送付する際に、情報に添付する認証情報に公開鍵暗号方式の公開鍵及び秘密鍵を用いる、認証システムとしては、送り手側での設備は上記送り手の分のＩＣカードを（送り手自身の通信用コンピュータ或いは一時利用する通信用コンピュータに備えられたカードリーダに）セットしたものとし、受け手側での設備も上記受け手の分のＩＣカードを（受け手自身の通信用コンピュータ或いは一時利用する通信用コンピュータに備えられたカードリーダに）セットしたものとする。そして、送り手は、送り手の分のＩＣカードの秘密鍵から認証情報を作成し、この認証情報と送り手のＩＣカードに収容された公開鍵証明書とを、情報と共に受け手に送付する。一方、受け手は、受け手の分のＩＣカードに収容された公証機関の公開鍵を用いて、送り手の上記公開鍵証明書に含まれる送り手の公開鍵を認証し、認証された送り手の公開鍵と認証情報（例えばデジタル署名）で、送り手から送付された情報を認証する。

【０００９】

【発明の実施の形態】以下、図面を参照しながら本発明の実施形態を説明する。また、単に「公開鍵」というときは、送り手や受け手の分の個別の公開鍵を指し、公証機関の公開鍵は「公証機関の公開鍵」又は「ＣＡの公開鍵」と記して、公開鍵を区別する。先ず図２は、本発明の携帯可能情報記憶媒体１０の一例としてＩＣカードに一対の公開鍵１及び秘密鍵２、並びに公証機関の公開鍵５が収容されている事の説明図である。公開鍵１は、公証機関ＣＡの署名３と共に公開鍵証明書４という形態で収容される。携帯可能情報記憶媒体に収容される、秘密鍵２、公開鍵証明書４（公開鍵１等を含む）、及び公証機関の公開鍵５は、書換え属性を禁止する書換禁止属性を備えたものとしておくことが好ましい。書換禁止属性は少なくとも秘密鍵に備えることが好ましいが、公表される公開鍵証明書４及び公証機関の公開鍵５も改ざん防止のために書換禁止属性を備えることがより好ましい。書換禁止属性は、携帯可能情報記憶媒体を前記鍵等を読出専用メモリに収容したＲＯＭカードとすることでも可能であるが、ＣＰＵを内蔵するＩＣカードのＯＳ（オペレーティングシステム）の機能により書換禁止属性に設定することもできる。また、安全性確保の為に秘密鍵の内容を外部に読み出せなくする、外部への読出属性を禁止する外部読出禁止属性を秘密鍵には設定しておくと良い。この点で、ＣＰＵを内蔵し、ＣＰＵ経由でアクセス権を制御するＩＣカードを用いると都合が良い。しかも、原文６から暗号文７への暗号化のプロセスは、ＩＣカードから秘密鍵を取り出して行うのでなく、ＩＣカード１０に原文６を渡して、ＩＣカード１０内部で秘密鍵２を用いて暗号文７を作成出力することが、ＣＰＵを内蔵することで可能となる。また、当然であるが、秘密鍵には、前記書換禁止属性と共にこの外部読出禁止属性の両方を設定しておくことが好ましい。

【００１０】本発明の携帯可能情報記憶媒体は、収容する公開鍵暗号方式の秘密鍵及び公開鍵は、メッセージ認証とユーザ認証を行うデジタル署名に用いるもの、或いはメッセージ認証に用いるもの等でも良い。なお、デジタル署名としてはＲＳＡ署名法に用いる秘密鍵及び公開鍵等である。また、メッセージ認証としては、冗長暗号化法等で用いる秘密鍵及び公開鍵等である。ところで、携帯可能情報記憶媒体中には、公開鍵が、公証機関のデジタル署名を伴った公開鍵証明書として収容されており、また公証機関の公開鍵も収容されていることから、公証機関からオフラインで送り手及び受け手に渡す。なお、本発明の携帯可能情報記憶媒体には、収容された秘密鍵の所有者の氏名、公証機関が割り当てたＩＤ番号等も収容しておいても良い。

【００１１】次に、以上の様な携帯可能情報記憶媒体を用いて行う、認証方法、認証システムについて説明する。図４は、送り手である太郎が、受け手である次郎に或るメッセージを送付するときに認証情報としてデジタル署名を行う際に、送付する情報の内容を説明する説明図である。太郎は、ＣＡ（公証機関）から太郎の秘密鍵Ａと（太郎の公開鍵Ａを有する）公開鍵証明書ＡとＣＡの公開鍵の入ったＩＣカードＡを取得しておく。太郎は、送りたいメッセージとＩＣカードＡ中の太郎の秘密鍵Ａとから署名を作成する。そして、メッセージと、署名と、ＩＣカードＡから公開鍵証明書Ａを取り出して、これら三つを次郎に送る。なお、次郎側でも、ＣＡ（公証機関）から、太郎からメッセージが送られる事前又は事後に、次郎の秘密鍵Ｂと（次郎の公開鍵Ｂを有する）公開鍵証明書Ｂと、ＣＡの公開鍵の入ったＩＣカードＢを取得する。

【００１２】次に、図５は、次郎が受け取った情報から、太郎のメッセージを最終的に認証するまでの、手順の説明図である。先ず、次郎は、ＩＣカードＢに収容されているＣＡの公開鍵で、送られた公開鍵証明書Ａが真正であることを確認する。同図の矢印は、便宜上、紙ベースの印鑑証明書の確認の様に、印鑑証明書に捺印されている公的機関の印影の確認に次いで、印鑑証明書が証明する実印の印影の確認という手順と同様に、ＣＡの公開鍵からＣＡの署名を認証し、ＣＡの署名から（太郎の）公開鍵Ａを認証する様にしてあるが、図３によるデ

ジタル署名の認証方法の説明、及びデジタル署名とはメッセージ認証とユーザ認証との両方の認証であることを踏まえれば、「ＣＡの署名の認証」（公開鍵証明書Ａの発行者である公証機関に対するユーザー認証）及び「太郎の公開鍵Ａ」の認証（メッセージ認証）とは、同時並列的に行われるものである。すなわち、送られてきた公開鍵証明書Ａが真正であることの確認は、図３のデジタル署名の認証方法において、メッセージが送り手太郎の公開鍵に、送り手太郎の署名が公証機関の署名に置き換えたプロセスである。受け手次郎は、受け取った公開鍵証明書Ａ中の太郎の公開鍵Ａから圧縮文を作成し、また受け取った公開鍵証明書Ａ中のＣＡのデジタル署名を、次郎のＩＣカードＢ中に収容されているＣＡの公開鍵で復号化してもう一つの圧縮文を作り、これら二つの圧縮文が一致する事で、公開鍵証明書Ａとして受け取った太郎の公開鍵が改ざんされてなく真正なものであると認証する。そして、認証された（太郎の）公開鍵Ａで、太郎の署名を認証し、（太郎の）署名からメッセージを認証する。以上で、送られたメッセージが確かなもので有り、且つ太郎から送られたものであることを判断する。

【００１３】次に、図１は、以上の様な携帯可能情報記憶媒体、及び認証方法によって、ネットワークで認証を行う認証システムの説明図である。同図では、太郎と次郎とが互いにメッセージを送受するに先立ち、ＣＡ（公証機関）からそれぞれの秘密鍵等やＣＡの公開鍵が収容された携帯可能情報記憶媒体としてＩＣカードを、それぞれ事前に取得しておき、太郎から次郎にメッセージを送る際に、デジタル署名と、公開鍵証明書を添付して送り、次郎は次郎のＩＣカードからＣＡの公開鍵を用いて、メッセージを認証する一例の説明である。

【００１４】同図のネットワークの認証システムでは、イーサネット等によるローカルエリアネットワークであり、公証機関の認証サーバー２１には（太郎や次郎等の）公開鍵のデータベースが有り、さらにＩＣカード１０ａ、１０ｂを発行する為のＩＣカードリーダライタ２２を備えている。なお、ＩＣカードの発行申請及び配付の両方を郵送等のオフラインで行う場合は、認証サーバーはネットワーク接続不要だが、ＩＣカードの発行申請はオンラインで行い配布はオフラインで行う場合は、認証サーバーはネットワークに接続されている必要がある。そして、太郎の端末２３ａは、メッセージにデジタル署名等を添付して次郎等に送付でき、且つ次郎等からのメッセージの認証ができる様に、ＩＣカードリーダ２４ａを備え、ＩＣカードリーダ２４ａには、太郎の（秘密鍵や公証機関の公開鍵等を収容した）ＩＣカード１０ａがセットされる。また、次郎側の端末２３ｂも、太郎から等のメッセージの認証ができ、且つメッセージにデジタル署名等を添付して太郎等に送付できる様に、ＩＣカードリーダ２４ｂを備え、ＩＣカードリーダ２４ｂには、次郎の（秘密鍵や公証機関の公開鍵等を収容した）ＩＣカード１０ａがセットされる。

【００１５】①　先ず、最初のステップは、太郎及び次郎のそれぞれは、同一の公証機関に各自の公開鍵の登録申請を行う。同図では破線の矢印で示してある様に、この手続きはネットワークによらずに（オンラインでも良いが同図の場合は）郵送等のオフラインである。鍵はＲＳＡ署名法に用いる鍵で（秘密鍵及び公開鍵）である。公証機関は、申請を受けて、一対の鍵を生成し、公開鍵を公開鍵データベースに登録する。登録により、公証機関では太郎や次郎の公開鍵の正当性を保証でき、また重複発行を防止できる。登録するのは少なくとも公開鍵側のみで良い。なお、公証機関としては、その目的に応じて、例えば会社、都道府県単位の地方自治体、国などが役割を果たし得る。また、この公開鍵の登録申請は、公証機関の公開鍵を入手の申請でもある。

【００１６】②　次のステップは、公証機関から太郎及び次郎に、それぞれの、秘密鍵と、公開鍵及びその公開鍵に対する公証機関のデジタル署名を有する公開鍵証明書と、公証機関の公開鍵とを有する、ＩＣカードを、郵送等のオフラインで送付する。この過程で、太郎や次郎のそれぞれの公開鍵に対するそれぞれの証明書と、公証機関の公開鍵も、前記それぞれのＩＣカードに入れて太郎や次郎に送ってしまう。従って、前記①の公開鍵の登録申請は、公証機関の公開鍵の請求申請でもある。なお、メッセージの受け手である次郎は、少なくとも最初のメッセージを受ける時については、メッセージを受けた後（事後）に、公証機関に次郎自身の公開鍵の登録申請（公証機関の公開鍵の請求申請を含む）を行っても良い。

【００１７】③　そして、太郎は次郎に、太郎のデジタル署名付きのメッセージを、太郎の公開鍵証明書とともに、ネットワークで送る。太郎はＩＣカードリーダ２４ａに自分のＩＣカード１０ａをセットする。デジタル署名の作成方法は、先に説明した通りであり、秘密鍵を引出して、或いはＩＣカード内部で暗号化する等して作成する。なお、ＩＣカード自身を盗難された場合に悪用を防ぐために、収容された秘密鍵の使用、及び公開鍵証明書の読み出し等は、所有者のパスワードを設定しておけば良い。

【００１８】④　一方、メッセージを送られた次郎側では、公開鍵証明書を真正なものであることを認証するために、該証明書にある公証機関のデジタル署名を認証する為の、公証機関の公開鍵は、次郎のＩＣカード１０ｂに次郎の公開鍵及び秘密鍵等と共に収容されている、（太郎と同一の公証機関に関する）公証機関の公開鍵を用いる。なお、前述した如く、次郎が自分のＩＣカード１０ｂを公証機関から入手するは、太郎がメッセージが送られた後（事後）又は前（事前）のどちらでも良い。そして、次郎は、公証機関から入手した自分のＩＣカード１０ｂをカードリーダ２４ｂにセットして、該ＩＣカ

ード１０ｂに収容されている公証機関の公開鍵で、太郎から送られた公開鍵証明書にあった公証機関のデシダル署名を認証し、太郎の公開鍵を認証する。

⑤　次いで、次郎は、認証した太郎の公開鍵で、太郎のメッセージを認証する。

【００１９】本発明では以上の様に、ＣＡの公開鍵を受け手である次郎が入手するのに、送り手である太郎からメッセージが送られた都度、オンラインで公証機関にＣＡの公開鍵を要求し、公証機関はオンラインで次郎にＣＡの公開鍵を送付するなどと言った面倒な手続きが不要である。すなわち、公表されるＣＡの公開鍵といえども、公証機関から次郎へＣＡの公開鍵をオンラインで送付する場合は、オンライン送付途中での第三者による改ざん防止の為に、該ＣＡの公開鍵がその公証機関のものに間違いない事を証明する為に、ＣＡの公開鍵に対する公開鍵証明書として送付する等の安全対策が必要となる。この公開鍵証明書は、該公証機関よりもより上位の上位公証機関で発行されるもので、下位公証機関のＣＡの公開鍵と、該ＣＡの公開鍵に対する上位公証機関のデジタル署名とからなる、ＣＡの公開鍵に対する証明書である。公証機関の上位、下位とは、例えば、会社に対しては地方自治体、地方自治体に対しては国等といった具合である。

【００２０】また、逆に、次郎から太郎にメッセージを送る場合は、太郎から次郎への場合と同様に、次郎は自分のＩＣカード１０ｂに収容されている次郎の秘密鍵、次郎の公開鍵に対する公開鍵証明書を用い、太郎は自分のＩＣカード１０ａに収容されている公証機関の公開鍵を用いることとなる。

【００２１】最後に、本発明により、デジタル署名として電子印鑑を、送り手太郎が送信するメッセージに捺印して、次郎にそのメッセージを含む送信データを送り、受け手次郎が電子印鑑を検印（認証）してメッセージを認証するまで一例を図６の説明図にまとめて示す。同図では、捺印者（太郎）のＩＣカードには、太郎のプライベートキーである太郎の秘密鍵と、ＣＡが発行した太郎の電子印鑑証明書と、ＣＡのパブリックキーであるＣＡの公開鍵が含まれている。太郎の電子印鑑証明書中には、太郎のパブリックキーである太郎の公開鍵（即ち太郎の電子印鑑）と、該公開鍵に対するＣＡのデジタル署名（電子印鑑の捺印）と、太郎の氏名及び太郎に付した番号等が含まれている。そして、太郎は、送るべきメッセージをハッシュ関数により圧縮して得たダイジェストを、太郎のプライベートキーである太郎の秘密鍵を用いて、公開鍵暗号方式により暗号化して得たものを、デジタル署名（太郎の電子印鑑の捺印）とする。なお、ハッシュ関数で圧縮したダイジェストは、元のデータに復元できないデータである。そして、太郎から次郎に送る送信データとしては、捺印対象のメッセージと共に、太郎の上記デジタル署名と、ＣＡ発行の捺印者太郎の電子印鑑証明書とを送る。一方、受け手であり検印者である次郎のＩＣカード中にも、次郎のプライベートキーである次郎の秘密鍵と、ＣＡが発行した次郎の電子印鑑証明書と、ＣＡのパブリックキーであるＣＡの公開鍵が含まれている。次郎の電子印鑑証明書中にも、次郎のパブリックキーである次郎の公開鍵（即ち次郎の電子印鑑）と、該公開鍵に対するＣＡのデジタル署名（電子印鑑の捺印）と、次郎の氏名及び次郎に付した番号等が含まれている。そして、次郎は受け取った前記送信データ中にある捺印者太郎の電子印鑑証明書中の、太郎のハプリックキーである公開鍵をハッシュ関数で圧縮してダイジェストを作る。一方、該電子印鑑証明書中のＣＡのデジタル署名を、次郎のＩＣカード中にあるＣＡのハプリックキーである公開鍵を用いて公開鍵暗号方式で復号化したものを前記ダイジェストと比較し、一致したならば、電子印鑑証明書中の太郎のハプリックキーである公開鍵を認証する。そして、認証された太郎のパブリックキーである公開鍵を用いて、公開鍵暗号方式で送信データ中の太郎のデジタル署名を復号化してダイジェストを作成し、一方、送信データ中のメッセージをハッシュ関数で圧縮してダイジェストを生成して、これら両ダイジェストを比較して一致したならば、メッセージを認証して、一連のプロセスが完了する。

【００２２】

【発明の効果】本発明によれば、認証に利用する各自の秘密鍵及び公開鍵、さらに公証機関による前記公開鍵の証明書、及び公証機関の公開鍵を安全に管理できる。これらを収容する携帯可能情報記憶媒体において、秘密鍵、そして公開鍵証明書や公証機関の公開鍵は書換禁止属性とすることで、より安全に鍵の管理ができる。更に、秘密鍵は外部読出禁止属性として媒体内部で暗号化することで、外部公表しない秘密鍵をより安全に管理できる。また、携帯可能情報記憶媒体中に鍵等が保管されているので、自分のネットワーク端末の磁気ディスク内等にこれら鍵等を保管する必要がなく、端末が他人に使用されて磁気ディスクに保管された鍵等を不正に盗用された、改ざんされる恐れが無い。携帯可能情報記憶媒体は、必要な時のみ端末のカードリーダにセットしておけば良く、後は自分で所持管理しておれば良い。従って、他のネットワーク端末でもこの携帯可能情報記憶媒体をセットすれば、情報を安全に送ることができる。また、鍵を磁気ディスクに収容して利用する従来の場合では、磁気ディスクに収容された状態を時間的に少なくする事で盗用や改ざんを防止する目的で、鍵が必要になる都度、公証機関に問い合わせして鍵を入手する使い方が望ましかった。しかし、本発明では、携帯可能情報記憶媒体内に安全に鍵を管理できるので、送り手側は毎回公証機関に毎回問い合わせする必要がなく、公証機関側としても最初に一回だけ携帯可能情報記憶媒体を本人に渡してしまえば済み、公証機関側での鍵運営も効率化でき

１１

る。また、公証機関の公開鍵も、各自の公開鍵及び秘密鍵と共に、携帯可能情報記憶媒体に収容しておくので、公証機関の公開鍵の必要の都度、公証機関にオンラインで請求・入手する等の面倒で安全対策の必要な手続きが不要である。従って、送り手から送られてきた公開鍵証明書中の公証機関のデジタル署名を、オフラインで認証し、すなわち公開鍵証明書をオフラインで認証し、送り手のメッセージ等の情報を認証することができる。

【図面の簡単な説明】

【図１】本発明の携帯可能情報記憶媒体を用いた認証システム、認証方法の説明図。

【図２】本発明の携帯可能情報記憶媒体が有する情報及び機能の一例の説明図。

【図３】デジタル署名の説明図。

【図４】本発明による情報伝達内容の説明図。

【図５】本発明による受け手側での認証の手順の説明図。

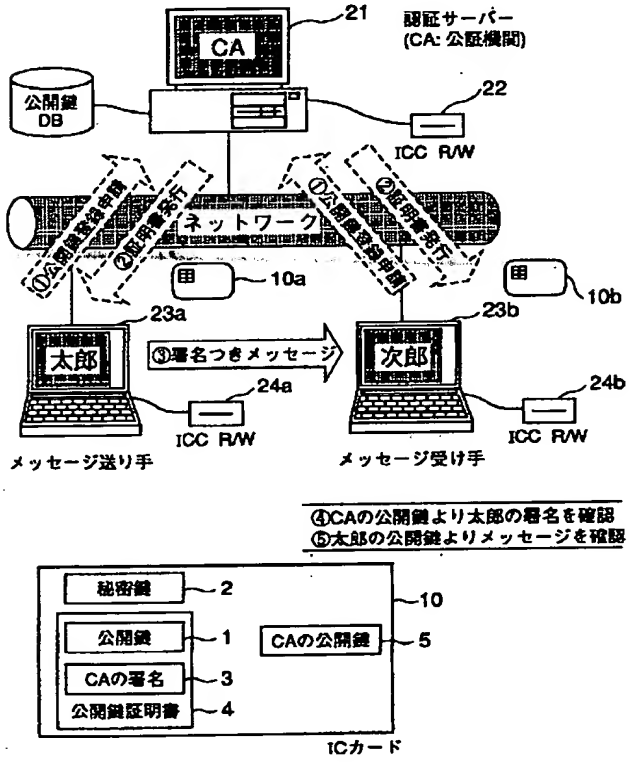
１２

【図６】本発明の一例として、デジタル署名（電子印鑑）の捺印から検印（認証）までの説明図。

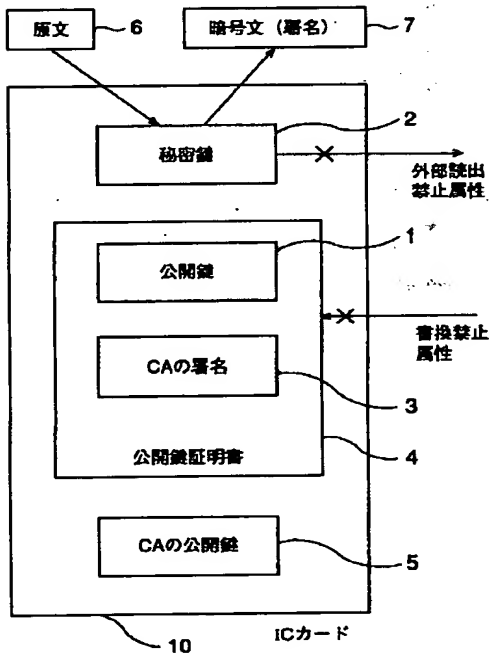
【符号の説明】

１　公開鍵
２　秘密鍵
３　公証機関（ＣＡ）のデジタル署名
４　公開鍵証明書
５　公証機関（ＣＡ）の公開鍵
６　原文（メッセージ等）
７　暗号文（デジタル署名等）
１０、１０ａ、１０ｂ　携帯可能情報記憶媒体（ＩＣカード等）
２１　認証サーバー
２２　カードリーダライタ
２３ａ、２３ｂ　端末
２４ａ、２４ｂ　カードリーダ

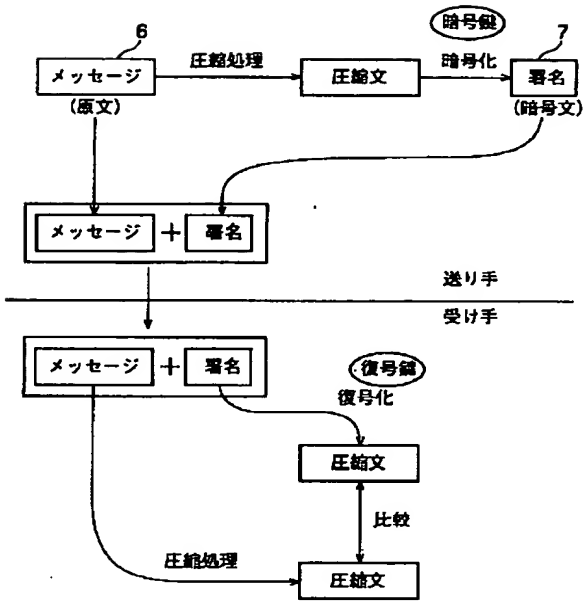
【図１】



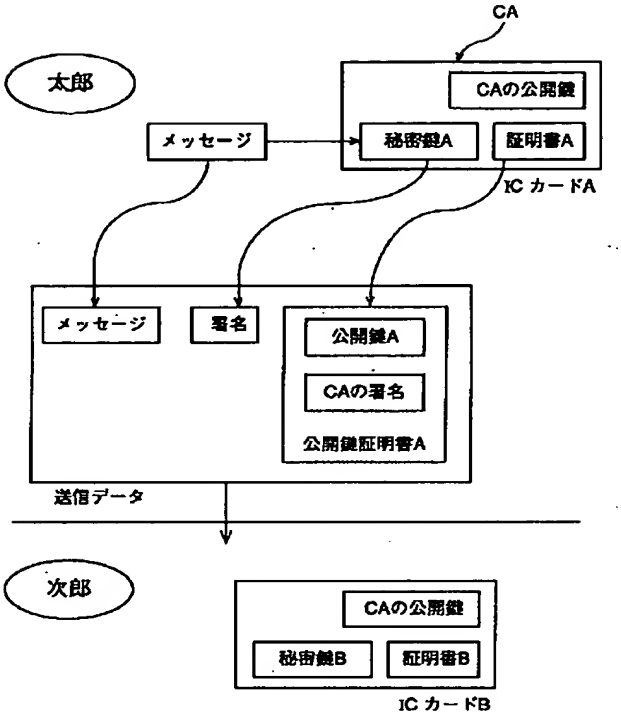
【図２】



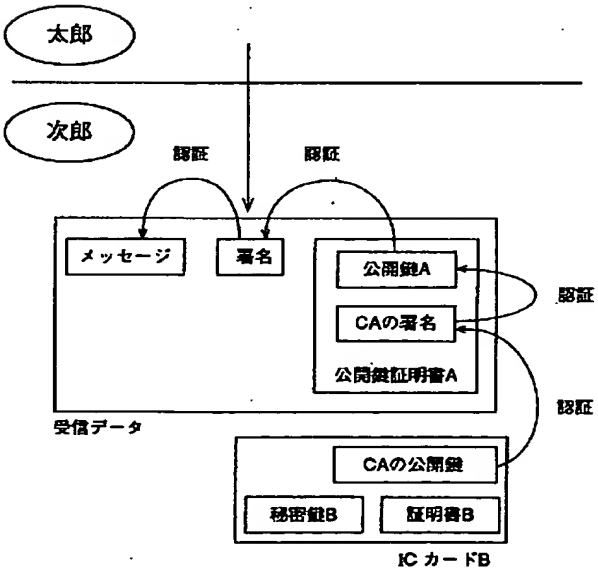
【図3】


6
メッセージ
（原文）
圧縮処理
圧縮文
暗号鍵
暗号化
7
署名
（暗号文）
メッセージ
＋
署名
送り手
受け手
メッセージ
＋
署名
復号鍵
復号化
圧縮文
比較
圧縮処理
圧縮文

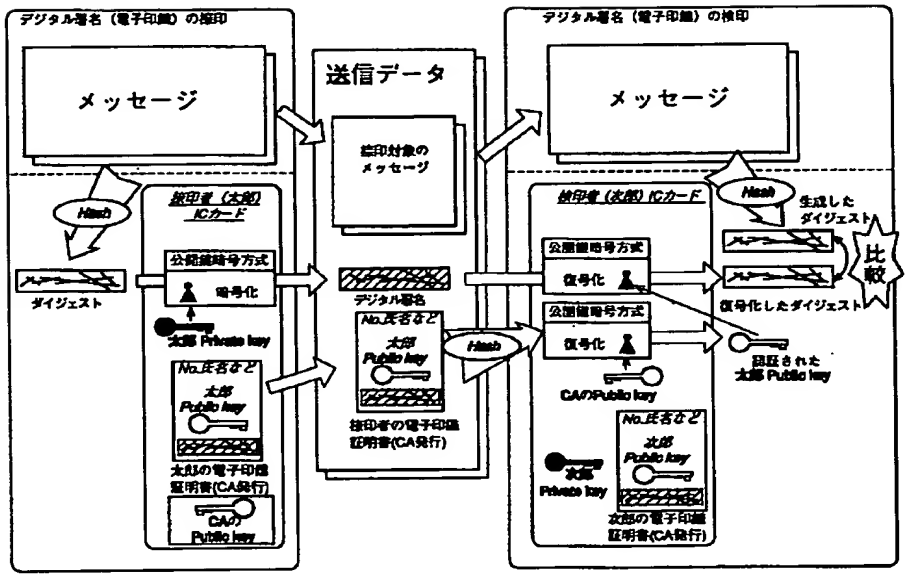
【図4】


CA
太郎
CAの公開鍵
メッセージ
秘密鍵A
証明書A
ICカードA
メッセージ
署名
公開鍵A
CAの署名
公開鍵証明書A
送信データ
次郎
CAの公開鍵
秘密鍵B
証明書B
ICカードB

【図5】


太郎
次郎
認証
認証
メッセージ
署名
公開鍵A
CAの署名
公開鍵証明書A
認証
認証
受信データ
CAの公開鍵
秘密鍵B
証明書B
ICカードB

【図6】


デジタル署名（電子印鑑）の捺印
メッセージ
Hash
ダイジェスト
捺印者（太郎）ICカード
公開鍵暗号方式
暗号化
太郎 Private key
No.氏名など
太郎 Public key
太郎の電子印鑑証明書(CA発行)
CAの Public key
送信データ
捺印対象のメッセージ
デジタル署名
No.氏名など
太郎 Public key
Hash
捺印者の電子印鑑証明書(CA発行)
デジタル署名（電子印鑑）の検印
メッセージ
検印者（次郎）ICカード
Hash
生成したダイジェスト
比較
公開鍵暗号方式
復号化
復号化したダイジェスト
公開鍵暗号方式
復号化
認証された太郎 Public key
CAのPublic key
次郎 Private key
No.氏名など
次郎 Public key
次郎の電子印鑑証明書(CA発行)